HB 4981 - House Committee on Criminal Justice
October 16, 2013

Automatic License Plate Readers (ALPR)

The ACLU of Michigan supports HB 4981. ALPR technology consists of high-speed cameras mounted on vehicles or stationary objects, such as telephone poles or overpasses. They photograph every license plate they encounter - capturing thousands of cars' information per minute – and use software to read the number and add a time and location stamp, and then record the information in a database. A computer checks the information in these pictures against police department databases. If a scanned plate matches information in the database, an officer is alerted. ALPR can be a useful tool for police officers, helping them recover stolen cars and arrest people with outstanding warrants. However, narrow guidelines must be implemented to protect our privacy.

Police departments around the country are rapidly expanding their use of automatic license plate readers to track the location of American drivers, but few have meaningful rules in place to protect drivers' privacy rights. The ACLU examined documents in 38 states from over 600 FOIA requests (ACLU report: You are Being Tracked, July, 2013) and discovered that local and federal law enforcement agencies are keeping innocent people's location information stored for years or even indefinitely, regardless of whether there is any suspicion of a crime.

License plate readers are used not only by police but also by private companies, which make their data available to police with little or no oversight or privacy protections. One of these private databases, run by a company called Vigilant Solutions, holds over 800 million license plate location records and is used by over 2,200 law enforcement agencies, including the U.S. Department of Homeland Security.

The spread of these scanners is creating what are, in effect, government location tracking systems recording the movements of many millions of innocent Americans in huge databases. We don't object to the use of these systems to flag cars that are stolen or belong to fugitives, but we believe there is a dire need for rules to make sure that this technology isn't used for unbridled government surveillance.

Training Materials

Few police departments place any substantial restrictions on how the ALPR's can be used. The approach in Pittsburg, Calif., is typical: a police policy document there says that license plate readers can be used for "any routine patrol operation or criminal investigation," adding, "Reasonable suspicion or probable cause is not required." While many police departments do prohibit police officers from using license

plate readers for personal uses such as tracking friends, these are the only restrictions. As New York's Scarsdale Police Department put it in one document, the use of license plate readers "is only limited by the officer's imagination."

Data Retention Policy

Policies on how long police keep plate-read data vary widely. Some departments delete records within days or weeks, some keep them for years, while others have no deletion policy at all, meaning they can retain them forever. For example, Minnesota State Patrol deletes records after 48 hours; Brookline, Mass., keeps records for 14 days; Burbank, IL for 21 days; Jacksonville, NC and Deerpark, NY for 30 days. Five states have passed laws prohibiting the police from retaining the license plate location records of innocent drivers for extended periods:

- Maine - 21 days
- New Hampshire - valid law enforcement purpose
- Arkansas - only for an on-going investigation
- Vermont - 18 months with restrictions
- Utah - 30 days for private entities and 9 months for law enforcement with restrictions

Huge databases don't lead to better law enforcement. A tiny fraction of the license plate scans are flagged as "hits." For example, in Maryland, for every million plates read, only 47 (0.005 percent) were potentially associated with a stolen car or a person wanted for a serious crime. Yet, many police departments are storing – for long periods of time – huge numbers of records on scanned plates that do not return hits. For example, as of August 2012:

- Jersey City, NJ, with a population of 250,000, has a database of 5 million plate reads and deletes data after 5 years.
- Grapevine, TX, with a population of 47,000, has a database of 2 million plate reads and has no policy on length of retention.
- Milpitas, CA, with a population of 67,000, has a database of 4.7 million plate reads and has no policy on length of retention.
- In contrast, the Minnesota State Patrol, covering a state with a population of 5.3 million, deletes non-hit data after 48 hours and has a database of fewer than 20,000 plate reads.

The government should not be storing data about people who are not even suspected of doing anything wrong, and the fact that some jurisdictions delete the records quickly shows that it is a completely reasonable and workable policy.

In our society, it is a core principle that the government does not invade its citizens' privacy and store information about their innocent activities just in case they do something wrong. Because location data can reveal extremely sensitive information about who we are and what we do, clear regulations must be put in place to keep the government from tracking our movements on a mass scale. While license plate readers can be used for legitimate law enforcement purposes, what the records revealed is astonishing: There are virtually no rules in place to prevent a system that can eventually track everybody all the time.

Recommendations

1. License plate readers may be used by law enforcement agencies only to investigate hits and in other circumstances in which law enforcement agents reasonably believe that the plate data are relevant to an ongoing criminal investigation.
2. The government must not store data about innocent people for any lengthy period. Unless plate data has been flagged, retention periods should be measured in days or weeks, not months and certainly not years.
3. People should be able to find out if plate data of vehicles registered to them are contained in a law enforcement agency's database.
4. Law enforcement agencies should not share license plate reader data with third parties that do not follow proper retention and access principles. They should also be transparent regarding with whom they share license plate reader data.
5. Any entity that uses license plate readers should be required to report its usage publicly on at least an annual basis.

Respectfully submitted,

Shelli Weisberg, Legislative Director
sweisberg@aclumich.org
248.535.7112

Automatic License Plate Readers

ACLU
AMERICAN CIVIL LIBERTIES UNION of MICHIGAN

A little noticed surveillance technology, designed to track the movements of passing drivers, is fast proliferating America's streets. Automatic license plate readers, mounted on police cars or on objects like road signs and bridges, use small, high-speed cameras to photograph every passing car.

The information captured by the readers – including the license plate number, and the date, time, and location of every scan – is being collected and sometimes pooled into regional sharing systems. Virtually all of the data license plate readers gather is of innocent people, not just of people suspected of crimes. As a result, enormous databases of innocent motorists' location information are growing rapidly. This information is often retained for years or even indefinitely, with few or no restrictions to protect privacy rights.[1]

License plate readers can serve an important and legitimate law enforcement purpose when they alert police to the location of a car associated with a criminal investigation. But such instances account for a tiny fraction of license plate scans, and many police departments across the country are storing millions of records about innocent drivers. Fortunately, there are protections that can be put in place, through legislation and law enforcement agency policies, that both protect Michiganders' privacy rights and preserve the use of the technology for unobjectionable and beneficial law enforcement purposes.

Privacy Risks

Automatic license plate reader use creates many privacy concerns that reach across a number of different dimensions:

- Automatic license plate readers have the potential to create permanent records of virtually everywhere any of us has driven, transforming the consequences of leaving home to pursue private life, and opening up many opportunities for abuse.
- License plate reader information can be very revealing. While one snapshot at one point might not seem sensitive, as blankets of plate readers cover our streets, and as the government stores data for longer periods of time, the technology quickly morphs into a powerful tracking tool that can reveal extremely sensitive information about who we are and what we do. Including what friends, doctors, protests, political events, or churches a person may visit.
- When it comes to law enforcement agencies, there are too few rules in place to ensure that the police do not store data for long periods of time about innocent people. The government should not invade people's privacy and store information about citizens' innocent activities in the event that some day they do something wrong.

Additional Resources

The ACLU has done extensive research on the use of automatic license plate readers. Comprehensive reports, data and talking points can be found at www.aclu.org/plates

Michigan's Role

Because of the privacy implications associated with the increased use of automatic license plate readers by law enforcement and private companies, the ACLU recommends legislation to regulate the use of the technology in Michigan. Our recommendations adhere to the following principles:

- **License plate readers may be used by law enforcement agencies only** to investigate hits and in other circumstances in which law enforcement agents reasonably believe that the plate data is relevant to an ongoing criminal investigation.
- **The government must not store data about innocent people** for any lengthy period. Unless plate data has been flagged, retention periods should be measured in days or weeks, not months and certainly not years. This principle is *the key* to regulating license plate readers.
- **People should be able to find out if plate data of vehicles registered to them** are contained in a law enforcement agency's database.
- **Law enforcement agencies should not share license plate reader data** with third parties that do not follow proper retention and access principles. They should also be transparent regarding with whom they share license plate reader data.
- **Any entity that uses license plate readers should be required to report** its usage publicly on at least an annual basis.

Shelli Weisberg, Legislative Director
American Civil Liberties Union of Michigan
Cell: 248-535-7112
sweisberg@aclumich.org

[1] American Civil Liberties Union. "You are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements" 2013. https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf